SECURITY ASSESSMENT FOR IEEE 802.11 FAMILY OF STANDARDS

Dominika Šebestová
Bachelor (3), FEEC BUT
E-mail: xsebes21@vutbr.cz

Supervised by: Radek Fujdiak
E-mail: fujdiak@feec.vutbr.cz

Abstract: This paper deals with analysis of security of wireless networks. It describes software intended for testing the security, specifically tools for Linux distribution of KALI. Furthermore it focuses on practical testing on an experimental network, where the functionality and efficiency of tools using brute force attacks, weakness in protocols or human errors are tested.

Keywords: IEEE 802.11, wireless network security, Wi-fi KRACK, WPS, WPA, WPA2, KALI Linux

1 ÚVOD

Kvalitní zabezpečení protokolu 802.11 neboli Wi-fi, je v dnešní době nepostradatelné. S častějším využíváním bezdrátových zařízení, tedy i bezdrátových sítí, roste snaha obejít jejich zabezpečení. Signál se z antén šíří všemi směry, tedy i skrz plášť budov do veřejných prostor, kde je přístupný bez jakékoliv nutnosti fyzické manipulace se zařízeními. To a velká popularita používání útočníkům usnadnilo práci. Na otevřených sítích je snadné zachytávat veškerou komunikaci, s běžně dostupnými nástroji není problém získat přístup i do chráněné sítě, spousta domácností i firem zabezpečení podceňuje a neuvědomuje si, jaké riziko bezdrátová síť představuje. Proto se společně s rozvojem bezdrátových sítí vyvíjely i protokoly pro jejich zabezpečení. První metoda zabezpečení WEP (Wired Equivalent Privacy) se po letech používání ukázala jako nedostatečná a musela být rychle nahrazena novým protokolem, který by na několik let zajistil bezpečí přenášených dat. Těmito nástupci se staly WPA a WPA2 (Wi-Fi Protected Access), které přinesly vyšší zabezpečení a použití silnější kriptografie [1]. Pro lepší představu situace, je nutné si některé základní i pokročilé útoky vyzkoušet v praxi na experimentální síti. Zaměřit se přitom na různé úrovně nastavení zabezpečení routerů a na vliv uživatele na bezpečnost jeho sítě.

2 TESTOVÁNÍ EXPERIMENTÁLNÍ SÍTĚ

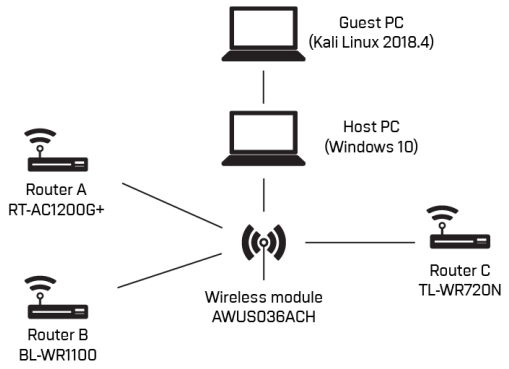
Pro testování byla zvolena linuxová distribuce KALI, určená pro penetrační testování, která běžela ve virtuálním prostředí. Prvním použitým nástrojem byl Airmon-ng určený pro přepnutí síťové karty do monitorovacího režimu - tj. když síťová karta přijímá veškerou komunikaci ve svém dosahu [2]. Airodump-ng je nástroj pro zachytávání paketů, díky němu je možné se podívat na všechny okolní sítě, zjistit jaký využívají kanál, jaké mají BSSID a SSID, tedy MAC adresu a název sízě. Defaultně přepíná mezi kanály rozsahu 2,4 GHz, proto je potřeba změnit jeho nastavení při monitoringu rozsahu 5 GHz. Komunikaci je možné sledovat v reálném čase a zároveň ji i ukládat do souboru pro pozdější analýzu [3]. Pokud uložená komunikace obsahuje 4-way handshake (vzájemné ověření klienta a routeru, probíhající ve 4 krocích) je možné s pomocí nástroje Crunch aplikovat offline útok hrubou silou a zkusit zjistit použité heslo. Pro testování útoku hrubou silou na PIN (Personal Identification Number) WPS (Wi-Fi Protected Setup), využívaný pro uživatelsky přívětivou konfiguraci routerů, je použit nástroj Reaver, díky rozmanitým možnostem nastavení je možné jej použít i v případě uzamknutí

přístupového bodu po několika neúspěšných pokusech [4]. Dále byl pak použit nástroj Krackattacks-scripts, ten umožňuje klienta otestovat sadou testů, které odhalí slabiny v implementaci, které by mohly zapříčinit úspěšné použití útoku na zařízení [5]. Posledním nástrojem je Fluxion pro Captive portal attack, útočníka provede všemi nutnými kroky od výběru sítě, za niž se bude vydávat falešný přístupový bod, po tvorbu certifikátu stránky a výběru vhodného rozhraní [6]. Pro realizaci testů, byl použit USB stick Alfa Network AWUS036ACH, s širokou podporou revizí protokolu 802.11, 2,4 GHz i 5 GHz s rozhraním USB 3.0.

Pro zjištění úrovně zabezpečení experimentální sítě funkčnosti jednotlivých nástrojů byl použit následně popsaný testovací scénář. Postupně bylo zkontrolováno zabezpečení přístupových bodů, úroveň zabezpečení klientů a poučenost uživatelů. Testování se odehrála na experimentální síti, představující domácí síť. Postup byl následovný, v prvním kroku se experiment zaměří na zabezpečení Wi-fi routerů. Ve Wiresharku byl zachycen jejich Beacon rámec, což je periodicky vysílaný rámec nesoucí informace o bezdrátové síti, a z něj bylo zjištěno použité zabezpečení. V další části budou dvě klientská zařízení otestována na náchylnost na případné provedení Wi-fi KRACK (Key Reinstallation Attacks). Routery zde nebyly testovány, jelikož nepodporují náchylné 802.11r. Ve třetí, poslední, části bude proveden útok využívající sociální inženýrství s cílem získat od uživatele heslo k síti.

2.1 Základní zabezpečení Wi-fi routerů

V experimentální sítí se nacházely tři Wi-fi routery, každý byl ukázkou odlišně starého a jinak zabezpečeného zařízení. S použitím programu Wireshark byl zjištěn používaný protokol zabezpečení. Router A byl zástupcem téměř správně zabezpečeného zařízení. Zachycený Beacon rámec ve Wiresharku prozradil, že je zabezpečený pomocí WPA2, ovšem má i aktivní WPS. I při znalosti délky hesla a všech znaků v něm obsažených by velikost slovníku byla 17 PB, WPS se u novějších zařízeních po třech neúspěšných pokusech uzamkne, délka útoku by tedy značně přesahovala standardní 4 hodiny. Router B, byl příkladem routeru se slabým heslem. Ve Wiresharku bylo ověřeno, že aktivním WPS nedisponuje. Pokračovalo se tedy další možností, zachycením a hrubým prolomením hesla z 4-way handshaku. Ten byl zachycen s pomocí nástroje airodump-ng a uložen do souboru s koncovkou .cap. Následně byl použit aircrack-ng pro útok hrubou silou, pro úsporu času byl slovník vygenerován podle hesla, i tak měl téměř 17 tisíc řádků. Třetí router, tedy router C měl, stejně jako první router, aktivní WPA2 i WPS. S přihlédnutím na stáří routeru však zabezpečení nefungovalo tak dobře, jako právě u prvního zařízení. Raver odhadl dobu lámání WPS na hodinu a půl, zvládl to však v ještě kratším čase. Zisk WPS vedl i k zisku hesla.



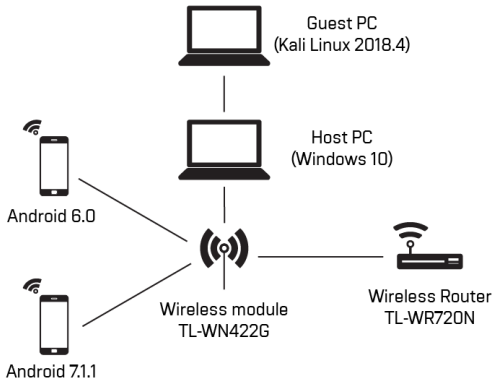
Obrázek 1: Experimentální síť pro testování routerů.

2.2 Náchylnost klientů na KRACK attack

Útok odhalil slabinu v protokolu WPA2, která nezávisí na lámání hesla hrubou silou. Slabinu obsahuje samotný standard, proto není závislá na konkrétním zařízení nebo implementaci. Využívá možnosti znovu odeslání třetí zprávy při 4-way handshaku, která klientovi říká, aby nainstaloval dohodnutý dočasný klíč PTK (Pairwise Transient Key). To umožní znovu použití odvozeného klíče pro šifrování a v případě zachycení zprávy se známým obsahem může být použitý klíč odvozen a použit pro dešifrovaní dat paketů. Aktuálně dostupné skripty neumožňují provedení útoky, pouze zařízení otestují na náchylnost. Testů je celkem šest:

1. Test zjišťuje, jestli klient přijímá opakovaně odeslané broadcastové ARP rámce, pokud by tomu tak bylo, zařízení je doporučeno aktualizovat (což u starších kusů není možné) další testy nemusí fungovat přesně.
2. Testuje zda klient nainstaluje GTK (Group Transient Key), tedy dočasný klíč pro skupinovou komunikaci, po group handshake.
3. Testuje, zda klient znovu instaluje GTK, při obdržení packetu s opakovaným označením.
4. Následující test ověřuje, jestli klient nainstaluje PTK po opakování 3. zprávy 4-way handshake.
5. Podobně jako 4. test, prvně zasílá infikovanou 1. zprávu, využívá slabinu kontrolního součtu MIC (Message Integrity Code), při použití TKIP, což je použitý šifrovací algoritmus pro WPA.
6. Test zjistí, zda klient instaluje GTK získaný v rámci opakovaného handshaku [7].

V rámci praktické části byly testováni dva klienti s operačním systémem Android 7.1.1. a Android 6.0. Zařízení s novějším systémem prošlo všemi testy, což znamená, že útok by na zařízení nešel vykonat, zařízení nepřijmá opakovanou 3. zprávu 4-way handshaku. Na starším telefonu by šel útok pravděpodobně snadno realizovat, jelikož zařízení projevilo náchylnost ve všech šesti testech.

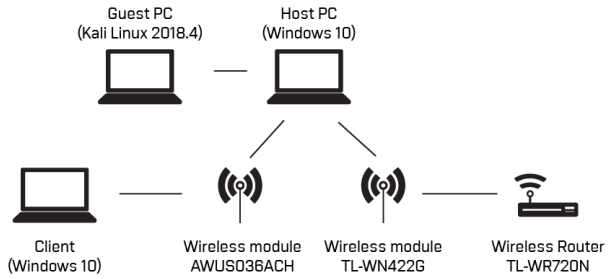


Obrázek 2: Experimentální síť pro sadu testů Krackattacks.

2.3 Captive Portal útok

Patří do kategorie útoků sociálního inženýrství, které cílí na lidské selhání, nejjednodušším příkladem je např. falešný přístupový bod - tedy nový přístupový bod s názvem sítě, která se v prostorách běžně využívá. Takový útok jde pak rozšířit a příkladem je program Fluxion, který využívá phishing

- falešnou webovou stránku pro zisk hesla nebo jiných citlivých údajů. K provedení tohoto testu byly potřeba dvě USB Wi-fi antény podporující injekční, monitorovací a master režim (dovoluje síťové kartě fungovat jako přístupový bod). Jedna je použita pro vytvoření falešné sítě a druhá pro zabránění komunikace mezi klientem a originální sítí. Po připojení klienta k falešné síti je pomocí DNS (Domain Name Server) zprávy přesměrován na web, tvářící se jako rozhraní routeru, kde je žádán o zadání hesla, to je porovnáno s dříve zachyceným handshakem.



Obrázek 3: Experimentální síť pro provedení Captive Portal attack.

3 ZÁVĚR

V práci byly prakticky otestovány mezery v zabezpečení bezdrátových sítí, také byly ověřeny výsledky dostupných nástrojů, na experimentální síti. V budoucnu budou tyto znalosti využity při tvorbě softwarového nástroje rozšiřujícího a sdružujícího některé nástroje z KALI Linuxu.

REFERENCE

[1] ARASH HABIBI LASHKARI, MIR MOHAMMAD SEYED DANESH a Behrang SAMADI. A survey on wireless security protocols (WEP, WPA and WPA2/802.11i). In: *2009 2nd IEEE International Conference on Computer Science and Information Technology* [online]. IEEE, 2009, 2009, s. 48-52 [cit. 2019-03-04]. DOI: 10.1109/ICCSIT.2009.5234856. ISBN 978-1-4244-4519-6. Dostupné z: <http://ieeexplore.ieee.org/document/5234856/>

[2] Airmon-ng. *Aircrack-ng* [online]. [cit. 2019-03-10]. Dostupné z: <www.aircrack-ng.org/doku.php?id=airmon-ng>

[3] Airodump-ng. *Aircrack-ng* [online]. [cit. 2019-03-10]. Dostupné z: <https://www.aircrack-ng.org/doku.php?id=airodump-ng>

[4] Reaver-wps-fork-t6x. *GitHub* [online]. [cit. 2019-03-10]. Dostupné z: <https://github.com/t6x/reaver-wps-fork-t6x>

[5] *Key Reinstallation Attacks: Breaking WPA2 by forcing nonce reuse* [online]. KU Leuven, 2017 [cit. 2018-11-28]. Dostupné z: <www.krackattacks.com>

[6] Fluxion. *GitHub* [online]. [cit. 2018-12-11]. Dostupné z: <www.github.com/FluxionNetwork/fluxion>

[7] Krackattacks-scripts. *GitHub* [online]. [cit. 2018-12-01]. Dostupné z: <www.github.com/vanhoefm/krackattacks-scripts>